UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/701,154	11/03/2003	Massimiliano Antonio Poletto	12221-014001	5561

26161   7590   01/08/2008

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER
MEHRMANESH, ELMIRA

ART UNIT	PAPER NUMBER
2113	

MAIL DATE	DELIVERY MODE
01/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

		Application No.	Applicant(s)	
Office Action Summary		10/701,154	POLETTO ET AL.	
		Examiner	**Art Unit**	
		Elmira Mehrmanesh	2113	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>25 October 2007</u>.

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1-3,5,7-16 and 18-27</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>1-3,5,7-16 and 18-27</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on <u>03 November 2003</u> is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some *   c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

This action is in response to a RCE filed on October 25, 2007 for the application

of Poletto et al., for a "Connection based anomaly detection" filed November 3, 2003.

Claims 1-3, 5, 7-16, 18-27 are pending in the application.

Claims 1, 5, 7, 14, and 16 have been amended.

Claims 4, 6, and 17 have been cancelled.

Claims 25-27 have been added.

Claims 1-3, 5, 7-16, 18-27 are rejected under 35 USC § 102.

Allowable Subject Matter

The indicated allowability of claims 23-24 is withdrawn in view of the newly

discovered reference(s) to Venkatraman (U.S. Patent No. 5,923,849). Rejections based

on the newly cited reference(s) follow.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b),
by another filed in the United States before the invention by the applicant for patent or (2) a
patent granted on an application for patent by another filed in the United States before the
invention by the applicant for patent, except that an international application filed under the treaty
defined in section 351(a) shall have the effects for purposes of this subsection of an application
filed in the United States only if the international application designated the United States and
was published under Article 21(2) of such treaty in the English language.

Claims 1-3, 5, 7-16, and 18-22 are rejected under 35 U.S.C. 102 (e) as being

anticipated by Ontiveros et al. (U.S. PGPub 20020107953).

As per claim 1, Ontiveros discloses a system, comprising:

a plurality of collector devices that are disposed to collect connection information to identify host connection pairs from packets that are sent between nodes on a network (paragraph [0024])

an aggregator device that receives the connection information from the plurality of collector devices (paragraph [0037]), and which produces a connection table that maps each node on the network to a record that stores information about packet traffic to or from the node (paragraph [0040]), with the aggregator device further comprising:

a process executed on the aggregator device to detect anomalies in connection patterns (paragraphs [0008] and [0024])

a process executed on the aggregator device to aggregate detected anomalies into the network events (paragraph [0026], Anomaly Detection System) with the anomalies that are detected including denial of service attack anomalies and scanning attack anomalies (paragraphs [0003] and [0024]).

As per claim 2, Ontiveros discloses the aggregator determines at least in part from the connection patterns derived from the connection table occurrences of network events (paragraph [0008], Intrusion Detection System).

As per claim 3, Ontiveros discloses the aggregator further comprises: a process that collect statistical information on packets that are sent between nodes on a network and which sends the statistical information to the aggregator (paragraph [0037]).

As per claim 5, Ontiveros discloses the collector devices have a passive link to devices in the network (Fig. 1).

As per claim 7, Ontiveros discloses the anomalies include unauthorized access and worm propagation (paragraphs [0003] and [0024]).

As per claims 8, Ontiveros discloses the connection table includes a plurality of records that are indexed by source address (paragraphs [0040] and [0044]).

As per claim 9, Ontiveros discloses the connection table includes a plurality of records that are indexed by destination address (paragraphs [0040] and [0045]).

As per claim 10, Ontiveros discloses the connection table includes a plurality of records that are indexed by time (paragraphs [0040] and [0049]).

As per claim 11, Ontiveros discloses the connection table includes a plurality of records that are indexed by source address, destination address and time (paragraphs [0040]-[0049]).

As per claim 12, Ontiveros discloses the connection table includes a plurality of connection sub-tables to track data at different time scales (paragraph [0042]).

As per claim 13, Ontiveros discloses the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table with each sub-table holding the sum of records received from all collectors during respective units of time (paragraphs [0042]-[0049]).

As per claim 14, Ontiveros discloses a method, comprises:

sending connection information to an aggregator to identify host connection pairs collected from a plurality of collector devices (paragraph [0024])

producing in the aggregator a connection table that maps each node on the network to a record that stores information about traffic to or from the node (paragraph [0040]), with the connection table including a plurality of entries that are indexed by source address (paragraphs [0040] and [0044]).

As per claim 15, Ontiveros discloses collecting statistical information in the collector devices to send to the aggregator device (paragraph [0024]).

As per claim 16, Ontiveros discloses determining from the connection information and the statistical information occurrences of network anomalies (paragraphs [0008] and [0024]); and aggregating anomalies into network events (paragraph [0026]) that indicate potential network intrusions (paragraph [0008], Intrusion Detection System) and

communicating occurrences of network events to an operator (paragraph [0057],

system administrator).

As per claim 18, Ontiveros discloses the connection table includes a plurality of

records that are indexed by destination address (paragraphs [0042] and [0045]).

As per claim 19, Ontiveros discloses the connection table includes a plurality of

records that are indexed by time (paragraphs [0040] and [0049]).

As per claim 20, Ontiveros discloses the connection table includes a plurality of

records that are indexed by source address, destination address and time (paragraphs

[0040]-[0049]).

As per claim 21, Ontiveros discloses the connection table includes a plurality of

connection sub-tables to track data at different time scales (paragraph [0042]).

As per claim 22, Ontiveros discloses the connection sub-tables include a time-

slice connection table that operates on a small unit of time and at least one other sub-

table that operates on a larger unit of time than the time slice sub-table with each sub-

table holding the sum of records received from all collectors during respective units of

time (paragraphs [0042]-[0049]).

Claims 23-27 are rejected under 35 U.S.C. 102(b) as being anticipated by Venkatraman (U.S. Patent No. 5,923,849).

As per claim 23, Venkatraman discloses a method of detecting a new host connecting to a network comprises: receiving statistics collected from a host in the network and indicating to a console that the host is a new host if, during a period of time T, the host transmits at least N packets and receives at least N packets, and if the host had never transmitted and received more than N packets in any previous period of time with a duration of T (col. 12, lines 10-15 and 33-39) and (col. 14, lines 39-53).

As per claim 24, Venkatraman discloses a method of detecting a failed host in a network comprises: determining if both a mean historical rate of server response packets from a host is greater than M, and a ratio of a standard deviation of historical rate of server response packets from the host to a mean profiled rate (col. 7, lines 41-50) of server response packets from the host is less than R over a period of time (col. 10, lines 25-47); and indicating the host as a potential failed host if both conditions are present (col. 7, lines 26-30) and (col. 14, lines 39-53).

As per claim 25, Venkatraman discloses indicating comprises: determining the minimal rate of N/T packets/second to avoid false positives caused by scans or spoofing attacks (col. 12, lines 16-25).

As per claim 26, Venkatraman discloses indicating comprises: determining a period seconds of continuous inactivity of the potential failed host to expire the potential failed host after the period of continuous inactivity; and generating a new host event if the expired failed host sends traffic on the network after the period of continuous inactivity has elapsed (col. 12, lines 16-25) and (col. 14, lines 39-53).

As per claim 27, Venkatraman discloses a host failure indicates an inability by the host to generate traffic on the network or an application failure (col. 12, lines 16-25).

Response to Arguments

Applicant's arguments have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Elmira Mehrmanesh whose telephone number is (571) 272-5531. The examiner can normally be reached on 8-4:30 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Robert W. Beausoliel can be reached on (571) 272-3645. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ROBERT BEAUSOLIEL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100